

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-272745

(43)公開日 平成8年(1996)10月18日

(51) Int.Cl. ⁵	識別記号	序内整理番号	F I	技術表示箇所
G 06 F 15/00	3 3 0	9364-5L	G 06 F 15/00	3 3 0 Z
G 09 C 1/00	6 3 0	7259-5J	G 09 C 1/00	6 3 0 B
	6 4 0	7259-5J		6 4 0 D
		7259-5J		6 4 0 A
	6 6 0	7259-5J		6 6 0 D

審査請求 未請求 請求項の数 3 OL (全 12 頁) 最終頁に続く

(21)出願番号 特願平7-280985

(22)出願日 平成7年(1995)10月27日

(31)優先権主張番号 特願平6-264201

(32)優先日 平6(1994)10月27日

(33)優先権主張国 日本 (JP)

(71)出願人 000005979

三菱商事株式会社

東京都千代田区丸の内2丁目6番3号

(72)発明者 斎藤 誠

東京都千代田区丸の内二丁目6番3号 三

菱商事株式会社内

(72)発明者 粉木 韶一

東京都千代田区丸の内二丁目6番3号 三

菱商事株式会社内

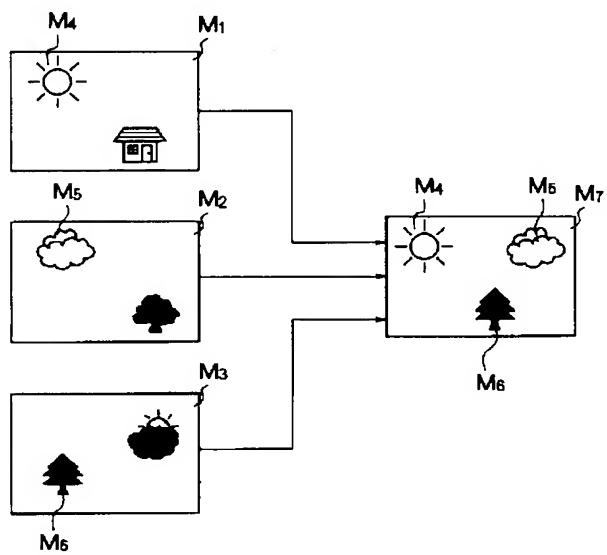
(74)代理人 弁理士 南條 健一郎

(54)【発明の名称】 データ著作権管理システム

(57)【要約】

【課題】 データベースシステムにおいて複数のデータを加工し、加工されたデータを供給するデータ著作権管理システムを提供する。

【解決手段】 データベースシステムにおける複数のデータの著作権を管理するシステムを提供する。データベースから入手した複数の暗号化されたデータを加工することにより新しいデータを作成し、暗号化して他人に供給する場合に、原材料である複数のデータの暗号鍵と、加工プロセスである加工プログラムにデジタル署名したデータを利用許可鍵として使用する。加工されたデータを受け取ったユーザが著作権管理センタにデジタル署名を提示して利用申込を行うと、著作権管理センタはデジタル署名に基づいて加工者を確認し、加工者が被加工データの正当なユーザであることが確認された場合にのみ、利用申込者に対して利用のための暗号鍵を提供する。



【特許請求の範囲】

【請求項 1】 複数の暗号化されたデータを加工することにより新しいデータを作成する場合のデータ著作権管理システムであって、前記データ著作権管理システムでは：データベースから入手した複数の暗号化されたデータをデータベースから供給された第 1 のユーザが暗号を用いて復号し；前記復号されたデータを加工することにより新しいデータを作成し；前記第 1 のユーザは前記複数の暗号化されたデータ各々の暗号鍵、デジタル署名された加工プログラムのデータを利用許可鍵として第 1 のユーザに供給し；加工され暗号化されたデータを受け取った前記第 2 のユーザがデジタル署名されたデータを著作権管理センタに提示して利用申込を行い；前記著作権管理センタはデジタル署名によって加工者である第 1 のユーザを確認し、加工者が第 1 のユーザであることが確認された場合に第 1 のユーザに対して利用のための暗号鍵を提供する。

【請求項 2】 データベース及び鍵管理センタを備え、1 次ユーザが入手した 1 次著作権データを加工し、加工によって得られた 2 次著作権データを 2 次利用者へ供給する場合に著作権を管理するデータ著作権管理システムであって：前記 1 次著作権データが 1 次利用鍵を用いて暗号化されて前記 1 次ユーザに供給され；前記 1 次著作権データの利用を希望する前記 1 次ユーザからの前記 1 次利用鍵の配布要求に対し、前記鍵管理センタが前記 1 次利用鍵を前記 1 次ユーザに配布し；前記 1 次ユーザは配布された前記 1 次利用鍵を用いて前記 1 次著作権データを平文化して 1 次利用を行い；前記 1 次著作権データの加工を希望する前記 1 次ユーザは前記鍵管理センタから前記 1 次著作権データを加工するための 2 次利用鍵の配布を受け、配布された前記第 2 利用鍵を用いて前記 1 次著作権データの加工を行い、加工中の著作権データは前記第 2 利用鍵を用いて暗号化されて保存され；加工が終了した前記 1 次ユーザは前記鍵管理センタから加工済みデータを配布するための第 3 暗号鍵の配布を受け、前記加工済みデータを前記第 3 暗号鍵を用いて暗号化して 2 次ユーザに供給し；前記 2 次著作権データの利用を希望する前記 2 次ユーザは前記鍵管理センタから前記第 3 暗号鍵の配布を受け、配布された前記第 3 暗号鍵を用いて前記 2 次著作権データを平文化して利用する；データ著作権管理システム。

【請求項 3】 前記 1 次ユーザによる前記 1 次著作権データの加工が、前記 1 次著作権データの複写物に対して行われる請求項 2 記載のデータ著作権管理システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明はデジタルデータの利用、すなわち表示(display)、保存(store)、複写(copy)、加工(edit)、転送(transmit)において著作権を管理するシステムに係るものであり、特にマルチメディアシ

ステムに対して用いることを考慮したものである。

【0002】

【従来の技術】 情報化時代と呼ばれる今日、これまで各々のコンピュータが独立して保存していた各種のデータを通信回線で各々のコンピュータを接続することによって相互に利用するデータベースシステムが普及しつつある。このデータベースシステムでこれまでに扱われてきた情報は古典的なコンピュータで処理することができる情報量が少ないコード化情報及びせいぜいのところでファクシミリ情報のようなモノクローム 2 値データであり、自然画及び動画のような情報量が格段に多いデータを扱うことができなかった。

【0003】 ところで、各種電気信号のデジタル処理技術が発展する中で、従来はアナログ信号としてのみ扱われていた 2 値データ以外の画像信号についてもデジタル処理技術の開発が進められている。この画像信号のデジタル化によりテレビジョン信号のような画像信号をコンピュータで扱うことが可能となるため、コンピュータが扱う各種のデータと画像信号をデジタル化した画像データとを同時に取り扱う「マルチメディアシステム」が将来の技術として注目されている。

【0004】 画像データは、文字データ及び音声データと比較して圧倒的に情報量が多いため、そのままで保存、転送あるいはコンピュータにおける各種の処理が困難である。そのため、これらの画像データを圧縮／伸張することが考えられ、いくつかの画像データ圧縮／伸張用の規格が作成されてきた。その中で、共通の規格としてこれまでに静止画像用の JPEG (Joint Photographic image coding Experts Group) 規格、テレビジョン会議用の H. 261 規格、画像蓄積用の MPEG 1 (Moving Picture image coding Experts Group 1) 規格及び現在のテレビジョン放送から高精細度テレビジョン放送に対応する MPEG 2 規格が作成された。これらの技術により、デジタル映像データのリアルタイム処理が可能となってきた。

【0005】 従来広く普及しているアナログデータは保存、複写、加工、転送をする毎に品質が劣化するため、これらの作業によって生じる著作権の処理は大きな問題とはならなかった。しかし、デジタルデータは保存、複写、加工、転送を繰り返しても品質劣化が生じないため、これらの作業によって生じる著作権の処理は大きな問題である。これまで、デジタルデータの著作権処理には的確な方法がなく、著作権法あるいは契約で処理されており、著作権法においてもデジタル方式の録音・録画機器に対する補償金が制度化されているにすぎない。

【0006】 データベースの利用法は単にその内容を参照するだけでなく、通常は得たデータを保存、複写、加工することによって有効活用し、加工したデータを複写あるいは転送によって他人に譲渡したりさらにはデータ

ベースに対して転送し、新しいデータとして登録することが行われる。従来のデータベースシステムにおいては文字データのみが取り扱いの対象となっていたが、マルチメディアシステムにおいては、これまでデータベース化されていた文字等のデータに加えて、本来アナログデータである音声データ及び画像データがデジタル化されてデータベースとされる。

【0007】このような状況において、データベース化されたデータの著作権をどのように取扱うかが大きな問題となるが、これまでのところそのための著作権管理手段、特に、複写、加工、転送等の2次利用について完成された著作権管理手段はない。本発明者らは特開平6-46419号及び特開平6-141004号で公衆電話回線を通じて鍵管理センタから許可鍵(permit key)を入手することによって著作権管理を行うシステムを、特開平6-132916号でそのための装置を提案した。

【0008】また、特願平6-64889号において、これらの上記先願発明をさらに発展させることによって、デジタル映像のリアルタイム送信も含むデータベースシステムにおけるデジタルデータの表示(音声化を含む)、保存等の1次利用及び複写、加工、転送等の2次利用における著作権管理方法を提案した。

【0009】この先願のデータベース著作権管理方法は、著作権の管理を行うために、データベースシステムにおいて、利用申し込み者に対して送信する利用を許可する鍵の他に、著作権を管理するためのプログラム、著作権情報を用いる。著作権管理プログラムは申し込みあるいは許可内容に反する利用が行われないように監視し管理を行う。

【0010】また、本発明者らは先願である上記特願平6-64889号において提案されたデータベース著作権管理方法を、具体的に実施したシステムであるデータベース著作権管理システムを特願平6-237673号において提案した。この特願平6-237673において提案したシステムは、データベース著作権管理システムを暗号鍵Kを管理する鍵管理センタ、データベース著作権を管理する著作権管理センタから構成し、データベースから配布されるデータは全て第1の暗号鍵K1によって暗号化(encrypt)され、データベースから直接にデータを利用する1次ユーザは、鍵管理センタに対して1次ユーザの情報I1を提示して利用形態に対応する鍵Kの要求を行い、1次ユーザから1次利用申込を受けた鍵管理センタは1次ユーザの情報I1を著作権管理センタに転送し、1次ユーザの情報を受け取った著作権管理センタはこの情報I1とともに著作権管理プログラムPcを鍵管理センタに転送し、著作権管理プログラムPcを受け取った鍵管理センタは著作権管理プログラムPcと利用形態に対応する第1の暗号鍵(cryptkey)K1、第2の暗号鍵K2を1次ユーザに対して通信ネットワーク

を経由して転送し、第1の暗号鍵を受け取った1次ユーザは受け取った第1の暗号鍵K1を用いてデータの暗号を解除(decrypt)して利用し、以後データの保存、コピーあるいは転送を行う場合には第2の暗号鍵K2を用いて暗号化及び復号化が行われる。

【0011】暗号技術においては、平文Mを暗号鍵Kを用いて暗号化し暗号文Cを得る場合を

$$C = E(K, M)$$

と表現し、暗号文Cを暗号鍵Kを用いて復号化し平文Mを得る場合を

$$M = D(K, C)$$

と表現するが、この明細書でも以後この表現を用いる。

【0012】データが保存されずに外部記憶媒体にコピーされたとき及び転送されたときには第1暗号鍵K1及び第2暗号鍵K2は廃棄され、1次ユーザが再度データを利用する場合には著作権管理センタから第1暗号鍵K1と第2暗号鍵K2の再交付を受け、この第2暗号鍵K2の再交付を受けたことにより、2次ユーザへのデータのコピーあるいは転送が行われたことが確認され、このことが著作権管理センタに記録される。

【0013】2次ユーザは著作権管理センタへの2次利用申込のときに1次ユーザの情報I1及び原著作権についての情報I0を著作権管理センタに提示する。著作権管理センタは利用形態に対応する許可鍵Kpとともに暗号化された第2暗号鍵(視聴許可鍵)K2及び第3暗号鍵(利用形態に対応した許可鍵)K3及び著作権管理プログラムPcを2次ユーザに送信する。

【0014】データの暗号化において用いられる代表的な手法として、秘密鍵暗号方式(Secret Key Crypto System)と、公開鍵暗号方式(Public Key Crypto System)がある。秘密鍵方式は、暗号化と復号化に同じ秘密鍵Ksを使用する暗号方式である。

$$C_{mks} = E(K_s, M)$$

$$M = D(K_s, C_{mks})$$

【0015】公開鍵暗号方式は、暗号化用の鍵が公開鍵(Public Key)Kbとして公開されており、復号化用の鍵が公開されていない暗号鍵方式であり、暗号化用の鍵は公開鍵と呼ばれ、復号化用の鍵は専用鍵(Private Key)Kvと呼ばれる。この暗号方式を使用するには、データを送信する側は暗号を受信する側の公開鍵Kbで暗号化し、

$$C_{mkb} = E(K_b, M)$$

データを受信する側は公開されていない専用鍵Kvで復号化する。

$$M = D(K_v, C_{mkb})$$

【0016】本発明者らは本件出願と同時に提出する出願において、ユーザが用意する第1公開鍵Kb1、第1公開鍵Kb1に対応する第1専用鍵Kv1、第2公開鍵Kb2、第2公開鍵Kb2に対応する第2専用鍵Kv2、データベース側が用意する第1秘密鍵Ks1及び第2秘密鍵Ks2を使

用し、データベース側では、データMを第1秘密鍵Ks1を用いて暗号化し、

$C_{mks1} = E(Ks1, M)$

第1秘密鍵Ks1をさらに第1公開鍵Kb1を用いて暗号化する

$C_{ks1kb1} = E(Kb1, Ks1)$

とともに、第2秘密鍵Ks2を第2公開鍵Kb2を用いて暗号化し、

$C_{ks2kb2} = E(Kb2, Ks2)$

これらの暗号化データ C_{mks1} 、暗号化第1秘密鍵及 C_{ks1} 及び暗号化第2秘密鍵 C_{ks2kb2} をユーザに送信する。

【0017】ユーザ側では、暗号化第1秘密鍵 C_{ks1kb1} を第1専用鍵Kv1を用いて復号化し、

$Ks1 = D(Kv1, C_{ks1kb1})$

復号化された第1秘密鍵Ks1を用いて暗号化データ C_{mks1} を復号化し

$M = D(Ks1, C_{mks1})$

利用するとともに、暗号化第2秘密鍵 C_{ks2kb2} を第2専用鍵Kv2で復号化し、

$Ks2 = D(Kv2, C_{ks2kb2})$

復号化された第2秘密鍵Ks2は復号化以降におけるデータの保存・複写・転送時の暗号鍵として使用する発明を提案している。

【0018】

【発明の概要】 ところで、上記特願平6-237673号等においてこれまでに提案されたデータベース著作権管理システムは利用されるデータあるいはデータベースが単一である場合を想定しており、複数のデータあるいはデータベースを利用して加工を行い新しいデータを作成することを想定していない。そこで、本件出願において単一のデータベースから得た複数のデータあるいは複数のデータベースから得た複数のデータを利用して加工を行い新しいデータを作成することを想定したデータ著作権管理システムを提案する。このシステムにおいては、データベースから入手した複数の暗号化されたデータを加工することにより新しいデータを作成し、暗号化して他人に供給する場合に、原材料である複数のデータ各々の暗号鍵と、加工プロセスである加工プログラムにデジタル署名したデータを利用許可鍵として使用する。

【0019】加工され暗号化されたデータを受け取ったユーザが著作権管理センタにデジタル署名したデータを提示して利用申込を行うと、著作権管理センタはデジタル署名によって加工者を確認し、加工者が被加工データの正当なユーザであることが確認された場合にのみ、利用申込者に対して利用のための鍵を提供する。

【0020】さらに別のシステムにおいては、第1暗号鍵を用いて暗号化されて供給された原データの利用を希望する1次ユーザは、鍵管理センタに1次利用鍵の配布を要求し、鍵管理センタは1次利用鍵を1次ユーザに配

布し、課金を行う。1次ユーザは1次利用鍵に含まれる第1暗号鍵を用いて暗号化データを復号化し利用するが、復号化データが1次ユーザの装置内へ保存される場合には1次利用鍵を用いて再暗号化される。データの加工を希望する1次ユーザはデータの加工を行うための2次利用鍵の配布を鍵管理センタに要求し、鍵管理センタは2次利用鍵を1次ユーザに配布する。2次利用鍵を受け取った1次ユーザは1次著作権データの複製を作成し、複製されたデータの加工を行い、加工途中の復号化2次データを2次利用鍵に含まれる第2暗号鍵により暗号化し、最終加工データは第3暗号鍵を用いて暗号化して1次ユーザの装置内に保存する。1次ユーザは2次著作権データのデータ加工についての二次著作権 (secondarily exploitation right) を行使するために鍵管理センタに第3暗号鍵を登録し、暗号2次データを第3暗号鍵を用いて暗号化して外部記憶媒体への複写あるいはネットワークシステムを介して転送することにより2次ユーザへ供給する。暗号化2次データの利用を希望する2次ユーザは、鍵管理センタに第3暗号鍵の配布を要求し、鍵管理センタは、第3暗号鍵を2次ユーザに配布する。2次暗号鍵を受け取った2次ユーザは2次暗号鍵を用いて暗号化2次データを復号し、利用する。

【0021】

【実施例】 図面を用いて本願発明の実施例を説明する。図1に示されたのは、本願発明に係るデータ著作権管理システムの構成図である。なお、このシステムにおいてデータベースに保管されているデータは暗号化されていない。先願である特願平6-237673号に示された実施例はデータを供給する手段としてデータベース以外に衛星放送あるいは記録媒体を使用している。これに対して、ここに示された実施例は説明を簡便にするためにデータを供給する手段としてデータベースだけを示す。しかし、本願発明がデータ供給手段としてデータベース以外に広告付き等の無料で暗号化する必要の無い衛星放送、地上波放送、CATV放送あるいは記録媒体を用いる場合にも適用可能なことは勿論のことである。

【0022】 1次ユーザが入手したデータをそのまま複写して2次ユーザに供給した場合には、そのデータに何等の変更も加えられていないため、そのデータに1次ユーザの著作権は発生しない。しかし、1次ユーザが入手したデータを基に新しいデータを作成した場合あるいは他のデータと組み合わせる等の手段を用いて新しいデータを作成した場合には、その新しいデータについて1次ユーザの2次著作権が発生する。また、2次ユーザが1次ユーザから入手したデータを基に新しいデータを作成した場合あるいは他のデータと組み合わせる等の手段を用いて新しいデータを作成した場合には、同様にその新しいデータについて2次ユーザの2次著作権が発生する。

【0023】 この図に示す実施例において、1, 2, 3

はテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、音声データあるいは映像データが暗号化されずに格納されたデータベースであり、9は通信事業者が提供する公衆回線あるいはケーブルテレビジョン事業者が提供するCATV回線等の通信回線、4は1次ユーザ端末装置、5は2次ユーザ端末装置、6は3次ユーザ端末装置、7はn次ユーザ端末装置である。また、8はデータ著作権を管理する著作権管理センタである。

【0024】これらのうちデータベース1、2、3、著作権管理センタ8、1次ユーザ端末装置4、2次ユーザ端末装置5、3次ユーザ端末装置6及びn次ユーザ端末装置7は通信回線9に接続されている。この図において、破線で示された経路は暗号化されたデータが伝送される経路であり、実線で示された経路は各ユーザ端末装置4、5、6、7から各データベース1、2、3及び著作権管理センタ8への要求が伝送される経路であり、1点鎖線で示された経路は各データベース1、2、3及び著作権管理センタ8から各ユーザ端末装置4、5、6、7へ利用形態に対応する許可鍵、著作権管理プログラム及び暗号鍵が送信される経路である。

【0025】本実施例においては、ユーザが用意する第1公開鍵Kb1、第1公開鍵Kb1に対応する第1専用鍵Kv1、第2公開鍵Kb2、第2公開鍵Kb2に対応する第2専用鍵Kv2、データベースが用意する第1秘密鍵Ks1、第2秘密鍵Ks2が使用される。データベースでは、データMを第1秘密鍵Ks1を用いて暗号化し、

$C_{mks1} = E(Ks1, M)$

第1秘密鍵Ks1を第1公開鍵Kb1を用いて暗号化する

$C_{ks1kb1} = E(Kb1, Ks1)$

とともに第2秘密鍵Ks2を第2公開鍵Kb2を用いて暗号化し、

$C_{ks2kb2} = E(Kb2, Ks2)$

これらの暗号化データ C_{mks1} 、暗号化第1秘密鍵 C_{ks1kb1} 及び暗号化第2秘密鍵 C_{ks2kb2} をユーザに送信する。

【0026】ユーザ側では、暗号化第1秘密鍵 C_{ks1kb1} を第1専用鍵Kv1を用いて復号化し、

$Ks1 = D(Kv1, C_{ks1kb1})$

復号化された第1秘密鍵Ks1を用いて暗号化データ C_{m1s1} を復号化して

$M = D(Ks1, C_{mks1})$

利用するとともに、暗号化第2秘密鍵 C_{ks2kb2} を第2専用鍵Kv2を用いて復号化し、

$Ks2 = D(Kv2, C_{ks2kb2})$

復号化された第2秘密鍵Ks2は復号化以降におけるデータの保存・複写・転送時の暗号鍵として使用される。

【0027】1次ユーザ4が入手したデータをそのまま複写して2次ユーザ5に供給した場合にはそのデータに何等の変更も加えられていないため、そのデータに1次ユーザ4の著作権は発生しない。しかし、1次ユーザ4

が入手したデータを基に新しいデータを作成した場合あるいは他のデータと組み合わせる等の手段を用いて新しいデータを作成した場合にはその新しいデータについて1次ユーザ4の2次的著作権が発生し、この1次ユーザはその2次的作品の原著作権者になる。同様に、2次ユーザ5が1次ユーザ4から入手したデータを基に新しいデータを作成した場合あるいは他のデータと組み合わせる等の手段を用いてさらに新しいデータを作成した場合には、同様にその新しいデータについて2次ユーザ5の2次的著作権が発生し、この2次ユーザ5はその2次的作品の原著作権者になる。

【0028】各データベース1、2、3にはテキストデータ、コンピュータグラフィックス画面あるいはコンピュータプログラムであるバイナリデータ、デジタル音声データ、デジタル映像データが格納されており、1次ユーザ端末装置4からの要求に対してデータ読み出し時に暗号化された状態で通信回線8を経由して1次ユーザ端末装置4に供給される。

【0029】データベースから入手するデータ著作権の管理は先願である特願平6-237673号に記載されている方法あるいは本件出願と同時に提出する出願に記載されている方法で行われる。

【0030】本発明者等が他の出願において提案した方法の概要を示す。暗号化方式として秘密鍵方式と公開鍵方式の両者を採用する。データの暗号化において公開鍵方式を採用すれば暗号化されたデータの安全性は向上するが、情報量の多いデータを公開鍵方式で暗号化した場合にはデータの復号化に要する時間が膨大なものとなり、実用的ではない。しかし、暗号に用いる鍵は人間が使用するものであるためその情報量はデータの情報量と異なりそれほど大きなものではない。

【0031】この著作権管理システムにおいては、ユーザが用意する第1公開鍵Kb1、第1公開鍵Kb1に対応する第1専用鍵Kv1、第2公開鍵Kb2、第2公開鍵Kb2に対応する第2専用鍵Kv2とデータベースが用意する第1秘密鍵Ks1及び第2秘密鍵Ks2が使用される。データベースでは、データMを第1秘密鍵Ks1を用いて暗号化し、

$C_{mks1} = E(Ks1, M)$

暗号化第1秘密鍵Ks1をさらに第1公開鍵Kb1を用いて暗号化する

$C_{ks1kb1} = E(Kb1, Ks1)$

とともに第2秘密鍵Ks2を第2公開鍵Kb2を用いて暗号化し、

$C_{ks2kb2} = E(Kb2, Ks2)$

これらの暗号化データ、暗号化第1秘密鍵 C_{ks1kb1} 及び暗号化第2秘密鍵 C_{ks2kb2} をユーザに転送する。ユーザ側では、暗号化第1秘密鍵 C_{ks1kb1} を第1専用鍵Kv1を用いて復号化し、

$Ks1 = D(Kv1, C_{ks1kb1})$

復号化第 1 密密鍵 K_{s1} で暗号化データ C_{mks1} を復号化して

$M = D (K_{s1}, C_{mks1})$

利用するとともに、暗号化第 2 密密鍵 C_{ks2kb2} を第 2 専用鍵 K_{v2} を用いて復号化し、

$K_{s2} = D (K_{v2}, C_{ks2kb2})$

復号化第 2 密密鍵 K_{s2} は復号化以降におけるデータの保存・複写・転送時の暗号鍵として使用される。

【0032】図 2 により、複数のデータを利用して加工を行い新しいデータを作成することについて説明する。この図に示されたように、1 次ユーザ 4 は単一のデータベースから入手したあるいは複数のデータベースから入手した複数の原データ $M1, M2, M3$ からデータを構成するパート $M4, M5, M6$ を抽出し、これらのパート $M4, M5, M6$ を利用して新しいデータ $M7$ を生成する。

【0033】このように生成された新しいデータ $M7$ を 1 次ユーザ 4 は 2 次ユーザ 5 に供給するが、新しいデータ $M7$ には 1 次ユーザ 4 が原データ $M1, M2, M3$ を加工することによって発生した 2 次的著作権の他に、データ $M7$ を生成するための原料であるパート $M4, M5, M6$ を得た原データ $M1, M2, M3$ についての原著作権も存在している。

【0034】これらの各原データ $M1, M2, M3$ は表示以外の利用すなわち保存、加工、複写あるいは転送が行われるときには各データとともに供給された第 2 密密鍵 K_{s2} で暗号化されるが、

$C_{m1ks2} = E (K_{s2}, M1)$

$C_{m2ks2} = E (K_{s2}, M2)$

$C_{m3ks2} = E (K_{s2}, M3)$

各々の原データの部品 $M4, M5, M6$ も同様に表示以外の利用が行われるときには各データとともに供給された第 2 密密鍵 K_{s2} で暗号化される。

$C_{m4ks2} = E (K_{s2}, M4)$

$C_{m5ks2} = E (K_{s2}, M5)$

$C_{m6ks2} = E (K_{s2}, M6)$

【0035】新しいデータは原データとデータの加工という行為から構成されている。コンピュータ技術においてデータの加工は原データとその加工プロセスによって表現される。そして、この原データと加工プロセスはコンピュータプログラムとコンピュータプログラム中に記載されたデータとして表現することができる。このようにプログラムとデータが一体化したものはオブジェクト (object) と呼ばれ、コンピュータでの処理をオブジェクト単位で行うオブジェクト指向技術 (object oriented technology) と呼ばれ、最近のコンピュータ技術における主流技術となっている。複数のデータから新しいデータを作成する技術はフレームワーク (frame work) あるいはシナリオと呼ばれ、代表的なものに Microsoft 社の「OLE」(ObjectLinking and Embedding) および Appl

e 社の「OpenDoc」がある。本発明では原データ相互の関係及び加工プロセスであるフレームワークあるいはシナリオを原データとともにオブジェクトとして扱う。

【0036】データ加工者である 1 次ユーザ 4 は加工プログラム P_e に第 1 専用鍵 K_{v1} を用いてデジタル署名を行い、

$S_{pe} = D (K_{v1}, P_e)$

デジタル署名された加工プログラム P_e とともに暗号化原データ部品 $C_{m4ks2}, C_{m5ks2}, C_{m6ks2}$ を 2 次ユーザ 5 に供給する。

【0037】デジタル署名された加工プログラム P_e とともに暗号化原データ部品 $C_{m4ks2}, C_{m5ks2}, C_{m6ks2}$ を受け取った 2 次ユーザ 5 は、著作権管理センタ 8 に対してデジタル署名が行われた加工プログラム P_e を提示して暗号化原データ部品 $C_{m4ks2}, C_{m5ks2}, C_{m6ks2}$ を復号化するための第 2 密密鍵 K_{s2} を要求する。

【0038】著作権管理センタ 8 は、第 1 公開鍵 K_{b1} を用いて提示された加工プログラム P_e のデジタル署名から 1 次ユーザ 4 を確認し、

$P_e = E (K_{b1}, S_{pe})$

その 1 次ユーザ 4 が第 2 密密鍵 K_{s2} を要求された原データの正当な利用者であることを確認し、その 1 次ユーザ 4 が正当な利用者である場合には第 2 密密鍵 K_{s2} を 2 次ユーザ 5 に転送する。しかし、その 1 次ユーザ 4 が正当な利用者でない場合には第 2 の秘密鍵 K_{s2} を 2 次ユーザ 5 に転送しない。

【0039】著作権管理センタ 8 に提示されたデジタル署名 S_{pe} には 2 次的著作権者であることを証明する正式な手続きとして著作権管理センタ 8 に登録される。

【0040】なお、1 次利用から n 次利用は永久に続くのではなく、データベース側あるいは原著作権者等の運用上の判断により適当な次数に止め、原著作物としてデータベースに強制的に登録するようにしてもよい。

【0041】図 3 により他の実施例を説明する。このシステムにおいては第 1 密密鍵 K_{s1} を含む 1 次利用鍵 K_1 、第 2 密密鍵 K_{s2} を含む 2 次利用鍵 K_2 、第 3 密密鍵 K_{s3} 、平文である原著作権ラベル L_{c1} 及び平文である著作権管理プログラム P_C が用いられる。図 3 に示されたデータ著作権管理システムは、データベース 11、鍵管理センタ 12、ユーザ 13、13、13... およびこれらを相互に接続するネットワーク 14 から構成されている。また、データベース 11 には情報提供者 (Information Provider: IP) 15、15、15... からデータが供給されるが、場合によってはデータベース 11 を経由することなく情報提供者 16、16、16... からネットワーク 14 を経由して直接にユーザ 13 に対してデータが供給されることがある。なお、本発明において利用されるデータはプログラムとデータが組み合わされたオブジェクトである。また、データベース 11 に

は情報提供者15, 15, 15...から1次ユーザ13にデータが供給されるが、場合によっては情報提供者16, 16, 16...からネットワーク14を経由してあるいはCD-ROM等の情報記録媒体17を介してデータベース11を経由することなく直接に1次ユーザ13に対してデータが供給されることもある。なお、この図において実線で示されたのは平文データ及び暗号鍵要求の経路、破線で示されたのは暗号化データの経路、1点鎖線で示されたのは暗号鍵の経路である。1次ユーザ13は単なる利用者ではなく入手した複数の原データを組み合わせたり、修正したりすることにより新しい著作物（2次著作物）を提供する情報提供者15あるいは16となりうる。

【0042】このように構成される本発明のデータ著作権管理システムにおいて、各情報提供者15, 16から提供される原データは著作権を保護するために暗号化されている。したがって、ユーザ13が入手した暗号化原データを利用するには暗号化原データを復号化しなければならない。このシステムにおいてはそのための暗号鍵はすべて鍵管理センタ12に預けられ、鍵管理センタ12が管理する。また、各情報提供者15, 16が採用する暗号方式は自由であるが、後で述べる2次利用以降で使用される暗号方式は鍵管理センタ12が採用する方式に限られる。

【0043】データベースからのデータ利用は一般的にパーソナルコンピュータを用いて行われるが、そこで用いられるOSとしてはセキュリティ対応処理を組み込んでいるものを使用する必要がある。また、暗号鍵等の管理を行うために著作権管理プログラムが使用されるが、この著作権管理プログラムおよび鍵管理センタ12から受け取った暗号鍵を保管しておく必要があるため、ソフトウェア的にメモリあるいはHDD上に実現される「キーカード」あるいは専用のボード、PCカード等でハードウェアとして実現される「キーカード」がこれらの保管場所として用意される。

【0044】鍵管理センタ12は、実際に利用されているか単に登録されているのみで利用されていないかを問わず、データ著作物の著作権の保護と著作権の利用に対する課金を行うために暗号鍵を保管し、保管されている暗号鍵と著作権ラベルの対応付けを行うことにより暗号鍵の管理を行う。

【0045】このシステムにおいて、平文である原データM0は第1秘密鍵Ks1を用いて暗号化され、
 $C_{m0ks1} = E(Ks1, M0)$

原著作権ラベルLc1とともに情報提供者15からデータベース11を介してネットワーク14を経由して、情報提供者16からネットワーク14を経由してあるいはCD-ROM等の情報記録媒体17を介して1次ユーザ13に供給される。

【0046】1次ユーザ13に供給される暗号化原データ

C_{m0ks1} には平文の原著作権ラベルLc0が付けられており、平文の原著作権ラベルLc0は1次利用鍵の入手等に利用される。すなわち、暗号化原データ C_{m0ks1} は平文原著作権ラベルLc0と暗号化原データ C_{m0ks1} から構成されている。平文原著作権ラベルLc0には原データの原著作者名、タイトル名、制作日等の一般情報の他に、使用しているアプリケーション・プログラム名、概要説明、使用料金及び課金方法等が記載されており、さらに必要に応じて利用鍵の番号が記載されている。なお、平文原著作権ラベルLc0に原著作権者によるデジタル署名を付しておけば虚偽の申告を防止することができる。

【0047】供給された暗号化原データ C_{m0ks1} の利用を希望する1次ユーザ13は、ネットワーク14を経由して鍵管理センタ12に原著作権ラベルLc1を提示して1次利用鍵K1の配布を要求する。

【0048】提示された1次著作権ラベルLc1により、配布すべき1次利用鍵が鍵K1であることを確認した鍵管理センタ12は確認された1次利用鍵K1をネットワークシステム14を経由して1次ユーザ13に配布する。配布された1次利用鍵K1を受信した時点で1次ユーザ13の装置は著作権管理モードになり、1次ユーザ13は1次著作権データの利用が可能になる。なお、第1秘密鍵Ks1は1次利用鍵K1に含まれているため、1次ユーザ13からは認識されない。一方、鍵管理センタ12は課金処理を行うとともに著作権データの使用状況および1次ユーザ13のデータベース利用状況を把握する。

【0049】1次ユーザ13は配布された1次利用鍵K1に含まれる第1秘密鍵Ks1を用いて暗号化1次著作権データ C_{m0ks1} を復号化し、
 $M0 = D(Ks1, C_{m0ks1})$

利用する。復号された原データM0が1次ユーザ13の装置内に保存される場合には第1秘密鍵Ks1を用いて再暗号化され、
 $C_{m0ks1} = E(Ks1, M0)$

暗号化原データ C_{m0ks1} が保存される。再暗号化された原データ C_{m0ks1} を再利用する場合には第1秘密鍵Ks1を用いて再復号化及び再暗号化が行われる。

【0050】原著作権データM0の加工を希望する1次ユーザ13はネットワーク14を経由して鍵管理センタ12に2次利用鍵K2の配布を要求する。

【0051】2次利用鍵K2の配布要求を受けた鍵管理センタ12は、ネットワーク14を経由して2次利用鍵K2を1次ユーザ13に配布する。2次利用鍵K2を受け取った1次ユーザ13は原データM0の加工を行い、途中加工データM0'を得る。途中加工データM0'がユーザ13の装置内に保存される場合には、第2秘密鍵Ks2によって暗号化される。

$C_{m0'ks2} = E(Ks2, M0')$

加工が最終的に終了すると、1次ユーザ13は最終加工

データM1についてのデータ加工に関する2次著作権を行使するために第3秘密鍵Ks3を用意し、第3秘密鍵Ks3を鍵管理センタ12に登録する。なお、第3秘密鍵Ks3は1次ユーザ13ではなく鍵管理センタ12が用意し、1次ユーザ13からの要求により配布するようにしてもよい。

【0052】1次ユーザ13が加工データM1を外部記憶媒体18への複写あるいはネットワーク14を介して転送する場合には、第3秘密鍵Ks3を用いて暗号化し、Cm1ks3=E(Ks3, M1)

2次ユーザ19へ供給する。

【0053】供給された暗号化加工データCm1ks3の利用を希望する2次ユーザ19は、鍵管理センタ12にネットワーク14を経由して第3秘密鍵Ks3の配布を要求する。2次ユーザ19からの第3秘密鍵Ks3の配布要求を受けた鍵管理センタ12は、ネットワーク14を経由して第3秘密鍵Ks3を2次ユーザ19に配布する。第3秘密鍵Ks3を受け取った2次ユーザ19は、第3秘密鍵Ks3を用いて暗号化加工データCm1ks3を復号化し、M1=D(Ks3, Cm1ks3)

利用する。その場合も、暗号化データCm1ks3を再度利用する場合には第3秘密鍵Ks3を用いて復号化および暗号化が行われる。

【0054】著作権管理プログラムPcが行う1次利用の制限について説明する。先願である特願平6-64889号に記載された発明と同様に、本願発明のデータ著作権管理システムにおいて入手され復号化されたデータの利用は通常の利用形態すなわちデータの直接的な利用およびその利用結果の印刷を含む出力に限定され、外部記憶媒体への複写あるいはネットワークシステムを経由しての転送及び加工、さらに原則としてデータの装置内部での保存を行うことはできない。なお、暗号化データの保存は可能である。また、使用中のアプリケーション・プログラムにより著作権主張がなされていないデータを表示・印刷・保存・複写・加工・転送することが可能なことはいうまでもない。

【0055】1次ユーザ13が外部の情報提供者15あるいは16から、直接にあるいはデータベース11を介して入手した暗号化原データCm0ks1はともに供給される原著作権ラベルLc0と組み合わされて1次ユーザ13の端末装置内のハードディスクドライブあるいは不揮発性メモリである保存装置に格納される。保存装置に格納されている暗号化原データCm0ks1の1次利用を希望する1次ユーザ13は平文の原著作権ラベルLc1を参照し、原データM0が使用しているアプリケーション・プログラム等の使用環境を確認する。

【0056】その結果、原データM0の利用が可能であると判断され、1次利用者13がこの原データM0を使用することを著作権管理プログラムPcに伝えると、著作権管理プログラムPcは原データM0が使用している

アプリケーション・プログラムを起動し、暗号化原データCm0ks1が保存装置から装置内の揮発性メモリに読み込まれる。その一方、1次著作権ラベルLc1が鍵管理センタ12に送られ、その結果、前に述べた処理フローにしたがい1次利用鍵K1が供給されると、暗号化原データCm0ks1が1次利用鍵K1に含まれている第1秘密鍵Ks1を用いて復号され、

M0=D(Ks1, Cm0ks1)

起動されたアプリケーション・プログラムによって利用することが可能となる。

【0057】1次ユーザ13の端末装置の揮発性メモリ上の復号化された原データM0を保存装置に保存する場合には第1秘密鍵Ks1を用いて暗号化して、

Cm0ks1=D(Ks1, M0)

保存が行われる。なお、この保存には、データ保全のための一時的ファイル(Temporaly File)の作成・保存も含まれる。再暗号化されたデータCm0ks1を再利用する場合には第1秘密鍵Ks1を用いて再復号化および再暗号化が行われる。また、1次利用鍵K1を使用している場合には、著作権管理プログラムPcにより復号化原データM0の表示・印刷及び暗号化原データCm0ks1の保存を行うことはできるが、その他の利用形態すなわち復号化原データM0の保存、加工、外部記憶媒体への複写、他の装置への転送、暗号化原データCm0ks1の外部記憶媒体への複写、他の装置への転送は禁止される。

【0058】したがって、原データM0の1部を切り出して他の一般データDに張り付けること(Cut & Paste)および一般データDの1部を切り出して原データM0に張り付けることも著作権管理プログラムPcによって禁止される。また、原データM0は第1秘密鍵Ks1を用いて暗号化された状態ならば例外的に保存装置に保存することができるが、何らかの加工が行われた場合に保存は禁止される。

【0059】著作権主張がなされている原データM0と著作権主張がなされていない一般データDとの区別及び原データM0が加工されたか否かは、著作権管理プログラムPcが判別する。この判別は、ファイル本体とともにコンピュータファイルを構成しているファイルの属性を記述した管理テーブルを調べることにより行われる。この管理テーブルにはファイルサイズ、作成日付に加えて著作権主張がなされていることを意味するフラグが記入されており、これらを調べることにより著作権主張がなされているか否か及びファイルの加工が行われたか否かが判別される。

【0060】保存装置に保存されているときに原データM0は暗号化原データCm0ks1として原著作権ラベルLc1と結合されているが、復号化されて揮発性メモリに読み込まれたときには著作権管理プログラムPcにより復号化原データM0と原著作権ラベルLc1は分離され、分離された著作権ラベルLc1は著作権管理プログラムPc

によって管理される。著作権管理プログラム P_c は原データ M_0 がどのアプリケーション・プログラムによって使用されているかを監視し、原データ M_0 の一般データ D への切り出し／張り付け及び一般データ D の原データ M_0 への切り出し／張り付けが行われることを禁止する。

【0061】著作権管理プログラム P_c が行うデータ加工の制限を説明する。1次利用の結果、原データ M_0 の加工を行うことを決定した1次ユーザ13は、原データ M_0 の加工を行うことをネットワーク14を経由して鍵管理センタ12に通知し、原データ M_0 の加工を行うための2次利用鍵 K_2 の配布を鍵管理センタ12に要求する。2次利用鍵 K_2 の配布要求を受けた鍵管理センタ12は2次利用鍵 K_2 をネットワークシステム14を経由して1次ユーザ13に配布する。このことにより1次ユーザ13の端末装置は加工モードになり、1次ユーザ13による原データ M_0 の加工が可能になる。

【0062】1次ユーザ13は暗号化原データ C_{m0ks1} を第1秘密鍵 K_{s1} を用いて復号化した上で表示装置に表示してデータの加工を行うが、初めに原データ M_0 を保護するために原データ M_0 の複写が行われ、この複写によって得られた加工用原データ M_0' に対して加工が行われる。この加工用原データ M_0' あるいはこの加工途中のデータ M_0'' を1次ユーザ13の端末装置内の保存装置に保存する場合には2次利用鍵 K_2 に含まれている第2秘密鍵 K_{s2} を用いて暗号化されて、

$C_{m0'ks2} = E(K_{s2}, M_0')$ または $C_{m0''ks2} = E(K_{s2}, M_0'')$

保存が行われる。暗号化原データ M_0 は加工されることなく保存装置内に保存されているため、その管理テーブルと加工途中のデータ M_0'' あるいは加工されたデータ M_1 のファイルサイズ、作成日付を調べることによりそのファイルが加工されたファイルであるか否かを判別することができる。

【0063】データの加工により複数の1次加工データ $M_{11}, M_{12}, M_{13} \dots$ が生成されるが、これらの1次加工データ $M_{11}, M_{12}, M_{13} \dots$ に1次ユーザ13の二次著作権が発生する。なお、これらの1次加工データ $M_{11}, M_{12}, M_{13} \dots$ は一次ユーザ端末装置の揮発性メモリ上にあるときには平文であるが、保存装置に保存されるときには第2秘密鍵 K_{s2} を用いて暗号化されて、

$C_{m11ks2} = E(K_{s2}, M_{11})$

$C_{m12ks2} = E(K_{s2}, M_{12})$

$C_{m13ks2} = E(K_{s2}, M_{13})$

・

・

・

【0064】これらの1次加工データ $M_{11}, M_{12}, M_{13} \dots$ についての二次著作権を行使するために、1次ユーザ13はネットワーク14を経由して鍵管理センタ12に第3秘密鍵 K_{s3} の配布を要求し、この配布要求に対して鍵管理センタ12は第3秘密鍵 K_{s3} を1次ユーザ13に配布する。第3秘密鍵 K_{s3} の配布を受けた1次ユーザ13は、平文あるいは復号された1次加工データ $M_{11}, M_{12}, M_{13} \dots$ を第3秘密鍵 K_{s3} を用いて暗号化し、

$C_{m11ks3} = E(K_{s3}, M_{11})$
 $C_{m12ks3} = E(K_{s3}, M_{12})$
 $C_{m13ks3} = E(K_{s3}, M_{13})$

・

・

・

1次ユーザ端末装置内の保存装置内に暗号化1次加工データ $C_{m11ks3}, C_{m12ks3}, C_{m13ks3} \dots$ が保存される。この暗号化データ $C_{m11ks3}, C_{m12ks3}, C_{m13ks3} \dots$ を利用する場合には第3秘密鍵 K_{s3} を用いて復号化および暗号化が行われる。

【0065】1次ユーザ13によって加工された1次加工データ $M_{11}, M_{12}, M_{13} \dots$ には、情報提供者が有する加工される前の原データ M_0 の一次著作権に加えて、データ加工についての1次ユーザ13の二次著作権が存在する。この二次著作権を行使するために1次ユーザ13は鍵管理センタ12に第3秘密鍵 K_{s3} とともに、データのタイトル名、使用しているアプリケーション・プログラム名、内容概要、1次著作権者名を送り、鍵管理センタ12は第3秘密鍵 K_{s3} とともに保管し、管理する。

【0066】一方、1次ユーザ13は暗号化1次加工データ $C_{m11ks3}, C_{m12ks3}, C_{m13ks3} \dots$ を外部記憶媒体18へ複写あるいはネットワーク14を介して転送することにより2次ユーザ19へ供給する。

【0067】供給された暗号化1次加工データ $C_{m11ks3}, C_{m12ks3}, C_{m13ks3} \dots$ の利用を希望する2次ユーザ19は、鍵管理センタ12に第3秘密鍵 K_{s3} を含む第3利用許可鍵 K_3 の配布を要求する。この第3利用許可鍵 K_3 による1次加工データ $M_{11}, M_{12}, M_{13} \dots$ の利用は、表示・印刷等の一般的な利用及びユーザ端末装置内の保存装置への保存に限定され、1次加工データ $M_{11}, M_{12}, M_{13} \dots$ あるいは暗号化1次加工データ $C_{m11ks3}, C_{m12ks3}, C_{m13ks3} \dots$ の外部記憶媒体18への複写あるいはネットワーク14を介しての3次ユーザへの転送及び1次加工データ $M_{11}, M_{12}, M_{13} \dots$ の再加工を行うことはできない。

【0068】前に述べたように、本発明において扱う著作権データはプログラムとデータが一体化した「オブジェクト」を対象としており、このオブジェクトはコンピュータプログラミングあるいは各種処理において部品的な取り扱いをすることができる。図4及び図3を用いて、オブジェクトである複数の原データを利用して新しい加工データを作る場合について説明する。図4において

て、31, 32, 33は各々オブジェクトとして構成された著作権主張がある原データM31, M32, M33であり、これらの原データM31, M32, M33を利用して新しい1次加工データM3030が作成される。原データM31, M32, M33の加工形態としては、34に示された1次加工データM34のようにその全部を利用する、35に示された1次加工データM35のようにその一部を利用するあるいは36に示された1次加工データM36のように修正して利用する、の3形態がある。

【0069】原データの加工は、オブジェクト単位で著作権データをリンクして引用して重ね合わせ／組み合わせを行うことにより加工処理が行われ、このような重ね合わせ及び組み合わせは自由に行うことができる。また、このように重ね合わせ／組み合わせが行われた1次加工データM3737にさらに他の事項を付け加えることもできる。このようにして新規に作成された1次加工データM3030はオブジェクトの集合体として構成されている。

【0070】前に述べたように、このようにして作成された1次加工データM30には原データM31, M32, M33の著作権の他に新たに加工についての1次ユーザ13の二次著作権が発生する。この1次ユーザ13の二次著作権を行使するためには1次加工データの暗号化が必要であり、そのために1次ユーザ13は各々の1次加工データM34, M35, M36に対応する第3秘密鍵Ks34, Ks34, Ks36を用意し、平文である1次加工データM34, M35, M36を各々対応する第3秘密鍵Ks34, Ks34, Ks36を用いて暗号化し、

$Cm34ks34 = E(Ks34, M34)$

$Cm35ks35 = E(Ks35, M35)$

$Cm36ks36 = E(Ks36, M36)$

外部記憶媒体18への複写あるいはネットワーク14を介して転送することにより2次ユーザ19へ供給する。また、第3秘密鍵Ks34, Ks34, Ks36を鍵管理センタ12に登録する。この第3秘密鍵の登録により、1次ユーザ13の二次著作権が鍵管理センタ12に登録される。

【0071】このとき1次ユーザ13から鍵管理センタ12に送られるのは、作成した複数の1次加工データの数に対応した複数個の第3秘密鍵Ks34, Ks35, Ks36の他に、第3秘密鍵の数、第2秘密鍵Ks24, Ks25, Ks26、原データ名、リンクしている他の原データの情報、使用した原データへのアクセスパス、原データM11, M12, M13が使用しているアプリケーションプログラム及び著作物概要説明等である。

【0072】複数個の第3秘密鍵Ks34, Ks35, Ks36を受けとった鍵管理センタ12は、原データ名、リンクしている他の原データの情報、使用した原データへの

アクセスパス、原データM11, M12, M13が使用しているアプリケーションプログラム及び著作物概要説明等を利用して複数の1次加工データに対応する著作権ラベルLc34, Lc35, Lc36を用意する。この時、新規作成の1次加工データM34, M35, M36と原データM11, M12, M13とのリンクが解除される。リンクが解除された時点で、それまでは1次加工データM34, M35, M36との間にリンク関係しか有していなかった原データの実体が、新規作成の1次加工データM34, M35, M36に埋め込まれ、このことにより2次ユーザ19へ供給された暗号化1次加工データCm34ks34, Cm35ks35, Cm36ks36の二次著作権の行使が可能となる。

【0073】供給された暗号化1次加工データ例えばM34の利用を希望する2次ユーザ19は、鍵管理センタ12に第3秘密鍵Ks34の配布を要求する。第3秘密鍵Ks34の配布要求を受けた鍵管理センタ12は、第3秘密鍵Ks34をネットワーク14を経由して2次ユーザ19に配布する。第3秘密鍵Ks34を受け取った2次ユーザ19は、第3秘密鍵Ks34を用いて暗号化1次加工データCm34ks34を復号化し、 $M34 = E(Ks34, Cm34ks34)$

を利用する。

【0074】なお、原データの著作権者あるいは1次加工データの著作権者は、鍵管理センタ12に申請することによりアクセスパスを変更することができる。また、原データの著作権者あるいは1次加工データの著作権者は、第3秘密鍵を用いてデータを加工（修正）することも可能であり、さらに、別の鍵を使用することも可能である。

【図面の簡単な説明】

【図1】 本発明実施例データベース著作権管理システムの構成図。

【図2】 オブジェクトである複数の著作権データを利用しての新しい著作権データ作成の説明図。

【図3】 本発明データ著作権処理システムの他の実施例の概要構成図。

【図4】 オブジェクトである複数の著作権データを利用しての新しい著作権データ作成の説明図。

【符号の説明】

1, 2, 3 データベース

8 著作権管理センタ

4, 5, 6, 7 ユーザ

9 通信回線

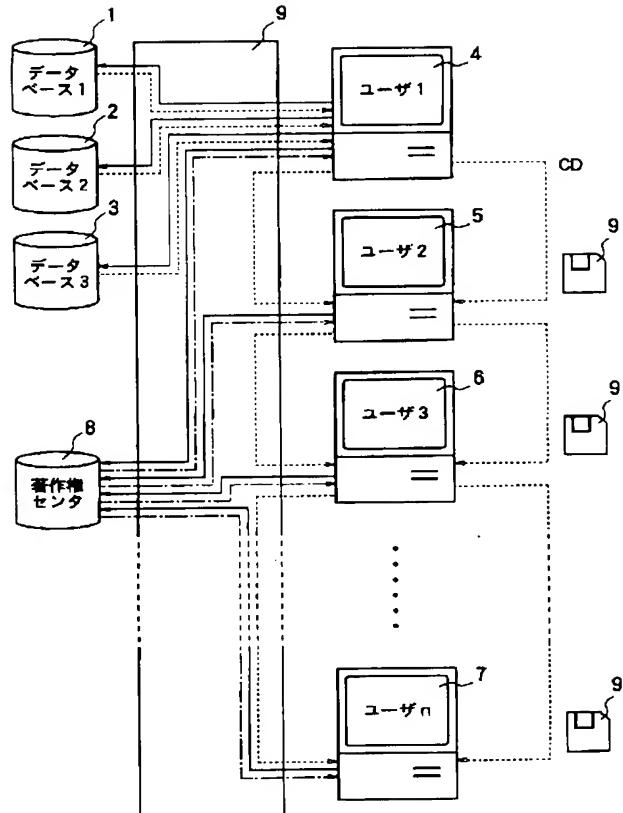
15, 16 情報提供者

17 情報記録媒体

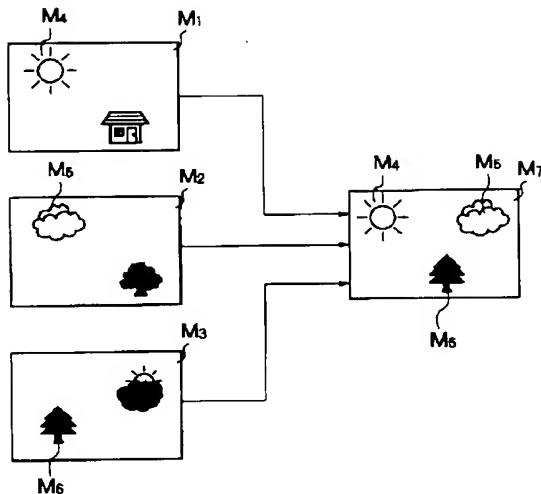
18 外部記憶媒体

19 2次ユーザ

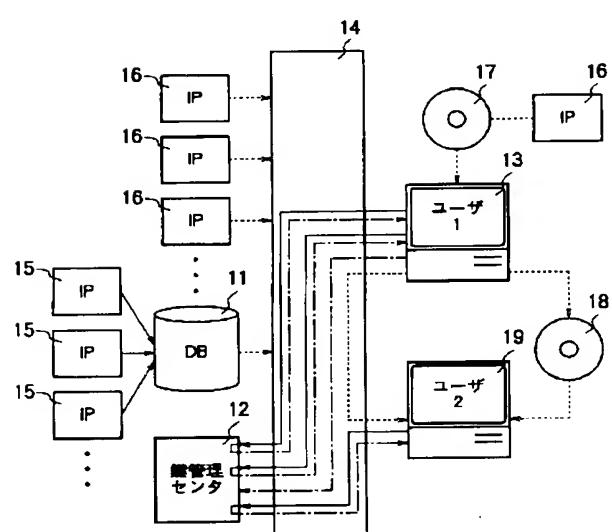
【図1】



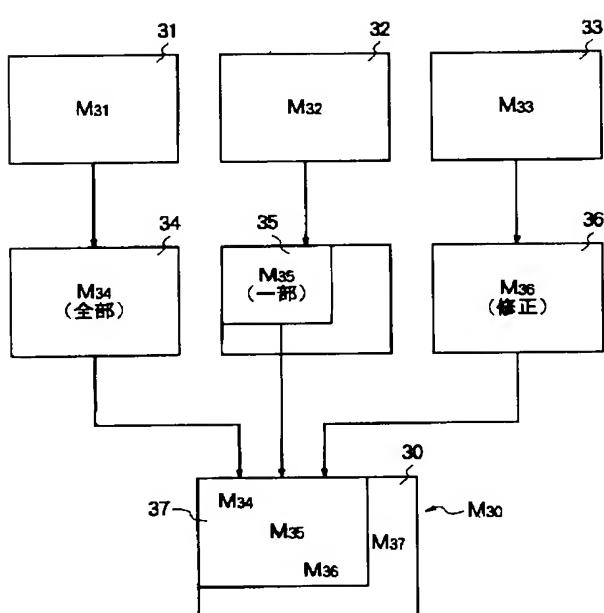
【図2】



【図3】



【図4】



フロントページの続き

(51) Int. Cl. 6	識別記号	庁内整理番号	F I	技術表示箇所
H 04 L 9/08		8842-5 J	H 04 N 1/44	
9/32			H 04 L 9/00	6 0 1 B
H 04 N 1/44		8842-5 J		6 7 5 A